



**Office of the Inspector-General of  
Intelligence and Security**

---

Annual Report

For the year ended 30 June 2018

---

Cheryl Gwyn  
**Inspector-General of Intelligence and Security**  
26 November 2018

## CONTENTS

|  |    |
|--|----|
| FOREWORD .....   | 2  |
| What has transparency meant in practice in this reporting year? .....  | 3  |
| ROLE OF THE INSPECTOR-GENERAL.....   | 6  |
| This reporting year .....  | 6  |
| <i>Legality and propriety</i> .....  | 6  |
| <i>Annual work programme</i> .....   | 6  |
| <i>New legislation – Intelligence and Security Act 2017</i> .....  | 6  |
| <i>Protected disclosures and disclosures under s 160 of the ISA</i> .....  | 8  |
| HOW EFFECTIVE IS OUR OVERSIGHT? .....  | 9  |
| Purpose of oversight .....   | 9  |
| <i>External purpose</i> .....  | 9  |
| <i>Internal purpose</i> .....  | 9  |
| Key requirements for effective oversight .....   | 10 |
| Measures of effectiveness .....  | 11 |
| <i>Breadth and depth of inspection and review work</i> .....   | 11 |
| <i>Time taken to complete inquiries and resolve complaints</i> .....   | 12 |
| <i>Extent to which agencies, Ministers and complainants accept and act on the<br/>Inspector-General’s findings and recommendations</i> ..... | 12 |
| <i>Extent to which agencies’ conduct, practices, policies and procedures change</i> .....  | 12 |
| Statutory advisory panel .....   | 13 |
| Intelligence and Security Committee.....   | 13 |
| THE YEAR AHEAD .....   | 14 |
| Work programme.....  | 14 |
| INQUIRY AND REVIEW POWERS .....  | 15 |
| Inquiries .....  | 15 |
| Operational reviews.....   | 15 |
| INQUIRIES AND REVIEWS CONCLUDED IN 2017/18 .....   | 16 |
| Review of the NZSIS handling of privileged communications and privileged information .....   | 16 |
| Review of the New Zealand security classification system.....  | 16 |
| Inquiry into complaints regarding alleged GCSB surveillance in relation to the South Pacific.....  | 17 |
| Review of NZSIS Requests made without warrants to financial service providers .....  | 18 |

|  |    |
|--|----|
| Review of the inadvertent collection of Advance Passenger Processing information in relation to Persons of Interest.....       | 18 |
| Inquiry into legality and propriety of warnings given by the NZSIS.....  | 18 |
| Review of the lawfulness of NZSIS access to data under the Customs and Excise Act and the Immigration Act 2009.....            | 19 |
| ONGOING INQUIRIES AND REVIEWS .....  | 20 |
| Inquiry into possible New Zealand engagement with Central Intelligence Agency (CIA) detention and interrogation 2001-2009..... | 20 |
| Review of a sample of NZSIS recommendations in respect of citizenship and immigration.....                                     | 20 |
| Review of sample of NZSIS security clearance decisions.....  | 21 |
| Afghanistan inquiry.....   | 21 |
| Review of warrants issued under the Intelligence and Security Act 2017 .....   | 21 |
| COMPLAINTS HANDLED BY THE OIGIS IN 2017/18.....  | 22 |
| Description of the complaints and inquiries.....   | 22 |
| WARRANTS AND AUTHORISATIONS .....  | 24 |
| GCSB.....  | 24 |
| NZSIS .....  | 25 |
| ASSESSMENT OF WHETHER COMPLIANCE SYSTEMS ARE SOUND.....  | 26 |
| Purpose of and approach to certification .....   | 26 |
| Outline and assessment of GCSB compliance systems.....   | 26 |
| <i>My assessment</i> .....   | 26 |
| <i>Compliance framework &amp; structure</i> .....  | 27 |
| <i>Compliance audit practices</i> .....  | 27 |
| <i>Self-reporting of incidents</i> .....   | 28 |
| <i>Interaction with IGIS office</i> .....  | 28 |
| Outline and assessment of NZSIS compliance systems .....   | 29 |
| <i>My assessment</i> .....   | 29 |
| <i>Compliance team</i> .....   | 30 |
| <i>Compliance reporting</i> .....  | 30 |
| <i>Audit programme</i> .....   | 30 |
| <i>Self-reporting of operational compliance incidents</i> .....  | 30 |
| <i>Interaction with IGIS Office</i> .....  | 30 |
| OTHER ACTIVITIES .....   | 32 |
| Intelligence Oversight Group .....   | 32 |
| Reference Group.....   | 32 |

|   |    |
|---|----|
| Visits to regional facilities .....             | 32 |
| Public engagements .....                        | 32 |
| Secondment .....                                | 33 |
| OFFICE FINANCES AND ADMINISTRATIVE SUPPORT..... | 34 |
| Funding .....                                   | 34 |
| 2017/18 budget and actual expenditure .....     | 34 |
| Administrative support .....                    | 34 |



## OFFICE OF THE INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

26 November 2018

Rt Hon Jacinda Ardern  
Prime Minister of New Zealand  
Minister for National Security and Intelligence

Dear Prime Minister

### **Annual Report 2017-2018**

I **enclose** my annual report for the period 1 July 2017 – 30 June 2018.

You are required, as soon as practicable, to present a copy of the report to the House of Representatives (s 222(3) of the Intelligence and Security Act 2017 (the Act), together with a statement as to whether any matter has been excluded from that copy of the report.

The Directors-General of the New Zealand Security Intelligence Service and the Government Communications Security Bureau have confirmed that publication of those parts of the report which relate to their agencies would not be prejudicial to the matters specified in s 222(4) of the Act, and that the report can be released unclassified without any redactions.

You are also required to provide the Leader of the Opposition with a copy of the report (s 222(5) of the Act).

As soon as practicable after the report is presented to the House I am required to make a copy publicly available on the Inspector-General's website.

With your concurrence, and in accordance with s 222(8) of the Act, I confirm my availability to discuss the contents of my report with the Intelligence and Security Committee when it next meets.

Yours sincerely

A handwritten signature in black ink, appearing to read 'C. Gwyn'.

Cheryl Gwyn  
**Inspector-General of Intelligence and Security**

**Copy to:** Hon Andrew Little  
Minister Responsible for the New Zealand Security Intelligence Service  
Minister Responsible for the Government Communications Security Bureau

## FOREWORD

If there was a theme to the work of my office in this reporting year it has been encouraging and demonstrating transparency.

Transparency is a core principle in my work as Inspector-General. Transparency is more than fashionable jargon: the intelligence and security agencies are departments of the public service and are publicly funded. The public has a right to know, to the extent possible, how this part of government is operating and that the agencies are operating within the law and with propriety.<sup>1</sup> Plainly, much needs to remain secret in order for the agencies to be effective, but that does not create a blanket of secrecy extending to all aspects of their work. Many things can properly be publicly said, and given my jurisdiction I am particularly interested in understanding and explaining the agencies' approach to their legal obligations and the way they interpret their powers.<sup>2</sup>

In addition, the intelligence agencies commonly use their special and intrusive powers to carry out their work in ways which encroach on fundamental human rights and would be unlawful without the specific authority they are given by legislation. In doing so, the agencies are not subject to the public scrutiny that applies to other government departments:

- The agencies are not, as a matter of course, accountable through the courts
- The Intelligence and Security Committee of Parliament provides parliamentary scrutiny of the agencies' policies, administration and expenditure, but it is a statutory committee, not a committee of Parliament as select committees are. This means it does not undertake a detailed scrutiny of bills in relation to the intelligence sector, or conduct inquiries with the associated investigative powers such as the ability to call for submissions and a requirement to report back to the House. Nor does it have a right of access to classified material and it may not inquire into any matter that is operationally sensitive
- The agencies are not subject to the full rigour of the Official Information Act or Privacy Act or to the Ombudsmen Act at all
- The secrecy of the agencies' operations means there is very little room for scrutiny by journalists, NGOs, or academics.

In our system the Office of the Inspector-General is the only external party that has full access to and insight into what the intelligence agencies are doing. My office in effect stands in the shoes of the public.

It was intended that the Intelligence and Security Act 2017 (ISA) would facilitate oversight of the agencies by the Inspector-General and enhance transparency.<sup>3</sup>

---

<sup>1</sup> "Propriety" is the word used in the Intelligence and Security Act 2017, s 156.

<sup>2</sup> There are developments within the agencies also, to engage more with the public and be more transparent. Both current Directors-General speak regularly at public events and give media interviews, and there is more detailed information available on the agencies' websites and in their annual reports than previously. Over the course of this year they have worked cooperatively with me in settling the operational detail that can be published in some of my significant reports.

<sup>3</sup> For example, ISA ss 17 and 153.

The ISA explicitly requires me to be transparent with my annual report and the reports of all my inquiries. Wherever possible I publish additional information, such as my annual work programme and review reports, even though this is not a statutory requirement.

I cannot force the agencies to implement my recommendations or to take any specific action. But transparency, in the form of public reporting, can often in itself spur positive change. The agencies do sometimes develop an added sense of urgency to address a report or implement a recommendation when an Inspector-General's report is about to be publicly released. And, to the extent that the concept of "effective" oversight assumes that appropriate changes and improvements will be made by the agencies as a result of the oversight body's work, my experience is that the Inspector-General's ability to publish is a vital tool in that process.

### **What has transparency meant in practice in this reporting year?**

This year I have published two inquiry reports.<sup>4</sup> I have also published five reports of IGIS reviews. I have tried to provide enough information for the public to be able to understand the general nature of the event or practice being examined; where something was in my view unlawful and/or improper, an explanation of what happened and why; my conclusions; and my recommendations for future policy and practice.

I acknowledge that some agency information cannot and should not be publicly released. To do so might harm national security interests, compromise operational activities or even the safety of staff, or unfairly or unlawfully affect privacy interests. But generally, large parts of my reports can be released to the public without harming those interests. In relation to all of my reports, I have worked with the Director-General of the relevant agency to avoid an unnecessarily conservative view about the detail of agency activities that can be published without prejudicing national security.

My report on how the Government Communications Security Bureau (GCSB) undertook intelligence activity in relation to New Zealand's interests in the South Pacific, *Complaints arising from reports of Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009-2015*, is a particular example of transparency. The level of detail about GCSB activities included in the report was a significant step towards giving the public meaningful information about the activities of the intelligence agencies.

My report on *Review of the New Zealand Classification System* will also, I hope, lead to better classification practice and greater transparency. The report examines New Zealand's system of classifying information and thereby protecting it from public scrutiny. It notes that classification systems have an inherent bias toward over-classification and recommends, amongst other things, a simplification of the system of classifying material in the first instance and a systematic programme of declassification of historic classified information.

My annual work programme was published in July 2018 to give the public a clear idea about the work we are intending to do over the course of the next reporting year.

---

<sup>4</sup> See summaries of these reports at pp 17-19 below.

When I released the work programme I noted my intention to report publicly on the intelligence warrants issued to the agencies during the first six to nine months of operation of the ISA. Parliament's and the public's expectation was that the changes introduced by the ISA would improve transparency around agency activity and accountability. The "triple lock" warrant system was intended to be a core protection for New Zealanders against improper intrusion on their privacy.

Our forthcoming report on warrants, *Warrants issued under the Intelligence and Security Act 2017*, looks at how the new warrant regime has been implemented so far and what issues and questions have arisen.

As well as introducing a new warrant regime, the ISA also provides for several new regimes to enable the agencies to access information held by other agencies. I touch on my office's role in overseeing these access arrangements below (see p 7).

The Deputy Inspector-General and I continued with our programme of public engagement. Speaking at public functions and giving media interviews is an important way of helping to foster public discussion about the role and activities of New Zealand's intelligence and security agencies and about public expectations of oversight. It is important that, as an oversight body, we are as transparent as we can be about who we are and what we do.

With that aim in mind, in April 2018 I set up an Inspector-General's "Reference Group". The Reference Group brings together a broad range of individuals and groups from outside government and the intelligence community. It deliberately represents a diversity of views and expert opinions that all, in one way or another, touch on the work of my office. There is little value in talking only to people who reinforce the views of my office or the views of the intelligence and security agencies. The purpose of the Reference Group is to help keep us in touch with legal, social and security developments in New Zealand and overseas, inform our thinking about our work programme and provide feedback on how we are performing our oversight role.<sup>5</sup> The members of the Group are not paid and do not have access to classified or otherwise sensitive information and nor is that necessary for them to fulfil a useful function.

The New Zealand IGIS office is a party to a Charter establishing the Five Eyes Intelligence Oversight and Review Council (FIORC), which comprises the non-political intelligence oversight and review bodies from the UK, USA, Canada, Australia and New Zealand. One of the purposes of FIORC is to encourage transparency to the largest extent possible and to enhance public trust. In this reporting year we met in Ottawa to discuss common issues in oversight.

Finally, in keeping with the theme of transparency, my office cooperated with a survey and ultimate report by Privacy International, a UK-based NGO, into intelligence sharing between governments.<sup>6</sup> This was consistent with our commitment to improving public knowledge, not just of what our

---

<sup>5</sup> The United Nations High Commissioner for Human Rights has recognised the importance of exposing oversight bodies to divergent points of view: see A/HRC/39/29, para 40.

<sup>6</sup> See <https://privacyinternational.org/report/1741/secret-global-surveillance-networks-intelligence-sharing-between-governments-and-need>

intelligence agencies do in New Zealand, but how they cooperate and share information with their overseas counterparts.

## ROLE OF THE INSPECTOR-GENERAL

### **This reporting year**

The Inspector-General oversees the two intelligence and security agencies, the New Zealand Security Intelligence Service (NZSIS or the Service) and the Government Communications Security Bureau (GCSB or the Bureau). I refer to them at times in this report simply as the agency or the agencies.

### **Legality and propriety**

The Inspector-General's statutory role<sup>7</sup> is to provide independent oversight of the agencies to ensure they act with propriety and operate lawfully and effectively.

The duty to ensure the agencies act lawfully requires the Inspector-General to form a view on what is the relevant legal standard in any particular situation and to measure the agencies' activities against that standard. It is implicit in the statutory duty to "ensure" their activities are lawful and proper that the agencies must treat the Inspector-General's opinion on any significant matter as authoritative or persuasive, in the absence of clear and relevant judicial authority, or a considered opinion from the Solicitor-General.<sup>8</sup>

"Propriety" is not defined in the ISA but is clearly intended to have a broader reach than specific questions of legality. It encompasses whether the agencies have acted in a way that a fully-informed and objective observer would consider appropriate and justifiable in the circumstances.

### **Annual work programme**

I prepare an annual work programme and I consult the Minister and the agencies on a draft before I finalise and publish it. Each year the work programme includes a mix of inquiries into specific complaints about the agencies, reviews of selected areas of their operations and inquiries into specific issues in the public interest or possible systemic problems.

### **New legislation – Intelligence and Security Act 2017**

The passage of new legislation governing the agencies' activities has necessarily had an impact on our work for much of the reporting period. A lot of our time has been devoted to implementation of ISA, both being consulted on draft agreements, policies and procedures and understanding the way in which the agencies were implementing the ISA.

The ISA established a new statutory regime for the issue of intelligence and other warrants to the GCSB and the NZSIS. The Act creates a single warrant regime for both agencies, replacing the separate

---

<sup>7</sup> Inspector-General of Intelligence and Security Act 1996 (IGIS Act), ss 4(a) and 11; ISA, s 156. The IGIS Act was the governing Act for part of the current reporting year. The ISA substantially took effect from 28 September 2017.

<sup>8</sup> In the context of a discussion about warrants under the ISA, referred to later in this report at pp 21 and 24-25, the Directors-General of the agencies have indicated that they do not agree with this conception of the Inspector-General's role but will seek advice on it.

and different warrant requirements that applied under the preceding legislation. As is often the case with new legislation, a lot of work goes into interpretation and application. That has certainly been the case here, both for the agencies themselves and for my office as the principal body overseeing the intelligence warrant process. I have reported in more detail on the issues specific to the new warrant regime in my report *Warrants issued under the Intelligence and Security Act 2017*.

The ISA also introduced several new regimes to enable the agencies to access information held by other agencies, through:

- Direct access to database information held by other agencies, under a direct access agreement (DAA) issued under the ISA by the Minister responsible for the holder agency and the Minister responsible for the intelligence and security agency
- Access to the business records of telecommunications network operators and financial service providers, under a new regime of business records approvals issued by the Minister responsible for the intelligence and security agency and business records directions issued by the Director-General of the intelligence and security agency
- Requests by the Director-General of an intelligence and security agency for voluntary disclosure of information which he or she believes on reasonable grounds is necessary for the agency to perform any of its functions.

The agencies consulted my office on the draft DAAs and on the draft business records authorisation structure. One of the issues we have discussed with the NZSIS, and will continue to monitor, is the need for it to have a framework or detailed statements of principle as to when it is necessary and appropriate to seek a warrant, issue a business records direction or make a request to another agency for voluntary disclosure of information. That framework or principles should reflect the level of intrusion on privacy interests and the degree of rigour and protection involved in each mechanism. Our *Review of NZSIS requests made without warrants to financial services providers*,<sup>9</sup> although conducted under the previous legislation, includes a recommendation to this effect.

The ISA also introduced the concept of Ministerial Policy Statements (MPSs)<sup>10</sup> to be issued by the Minister responsible for the agencies and govern how the intelligence and security agencies undertake various generally lawful activities.

The MPSs set out the guiding principles. These reflect the Minister's expectations about how the agencies should properly perform their functions, the limits of any activity and, generally speaking, the way in which it will be carried out. While the obligation on the agencies is merely to "have regard to" the MPSs, in essence they establish a framework for good decision-making and provide a measure to guide the Inspector-General's jurisdiction to ensure the agencies act "properly". The MPSs stipulate that the agencies must be able to justify any departures from the standards set out in them. Since the ISA came into effect our review and inquiry work has included assessing agency activity against the expectations in the relevant MPSs.

---

<sup>9</sup> See p 18 below.

<sup>10</sup> ISA, ss 206-216.

## Protected disclosures and disclosures under s 160 of the ISA

The ISA made changes to the protected disclosures regime which I referred to in my last annual report. The Inspector-General is now the ‘appropriate authority’ to receive protected disclosures about classified information or information relating to the activities of the intelligence and security agencies from employees of public sector organisations which hold such information.<sup>11</sup> The ISA carries over in s 160 the unique protection for employees of an intelligence and security agency who draw any matter to the attention of the Inspector-General that existed under the Inspector-General of Intelligence and Security Act 1996. The new Office of the Inspector-General of Intelligence and Security (OIGIS) policy for handling protected disclosures is on our website at [www.igis.govt.nz/publications/igis-policies/](http://www.igis.govt.nz/publications/igis-policies/).

During the reporting period, my office participated in the State Services Commission’s preliminary consultation about potential reform to the protected disclosures regime. There is scope for improvements to the legislation governing protected disclosures. But a legislative response is not the full answer, as I indicate below. During this period the NZSIS and GCSB developed a joint policy statement concerning protected disclosures. It is mandatory for an agency to have an internal policy concerning protected disclosures, and the agencies’ former policies were dated. I welcomed the agencies revisiting this matter and my office was consulted on the development of the policy statement. That process highlighted the tensions that are inherent in the intelligence and security context – not just in New Zealand – between encouraging and protecting those who make disclosures about serious wrongdoing, and guarding against the insider threat, ie the leaking of classified or sensitive information outside the mandated processes. I discussed with the agencies the importance of not conflating protected disclosures with protective security issues. The overwhelming experience from other foreign oversight agencies is that intelligence and security agencies will best protect their classified information and ensure staff loyalty when they have strong cultures, supported from the top, which actively encourage staff to voice concerns and complaints internally, and without recrimination.

---

<sup>11</sup> Protected Disclosures Act 2000, s 12.

## HOW EFFECTIVE IS OUR OVERSIGHT?

### Purpose of oversight

#### External purpose

The intelligence and security agencies have empowering mechanisms under their legislation to do a whole range of things which, if carried out by any other citizen, would constitute criminal offences. For example, a warrant can provide legal authority to covertly access computers, intercept phones and mail, or break into people's homes to plant listening devices or cameras.<sup>12</sup> They can also carry out activities which might be otherwise unlawful, but not criminal. For example, intelligence agencies can electronically track individuals, or obtain customer information from banks, or secretly follow individuals onto private property. They are permitted to encroach, if necessary, on New Zealanders' privacy rights by exchanging highly personal or other information with domestic and foreign intelligence and security and law enforcement agencies.

At the same time the secrecy of NZSIS and GCSB's activities, capabilities, and techniques inevitably makes it much more difficult for Parliament, the news media and the public at large to know what they do, form a view on it, and hold them to account as they can with other parts of the government or the public sector. This in turn can have a significant impact on the level of trust and understanding the public has in the value, role and effectiveness of the agencies.

In those circumstances external, independent and effective oversight is vital. That oversight function can only be exercised by people permitted to access the secret (classified) information the agencies gather, and to know the means by which they gather it. In New Zealand, apart from the Minister responsible for the agencies, the Prime Minister and a small handful of senior public servants, that external access is limited to the Commissioners of Intelligence Warrants (retired High Court Judges who, together with the Minister, have a role in authorising intelligence warrants) and the Office of the Inspector-General of Intelligence and Security.

Members of the public must be able to trust in the independence and integrity of the Inspector-General and his or her staff. The existence and public work of my office provides a form of indirect public view into the agencies themselves.

#### Internal purpose

Effective, independent oversight should also assist agency application of the law and minimise the risk of any illegality or impropriety in agency operations. It is important that the agencies, just like any other public bodies, operate according to best practice standards and in such a way as to give full effect to the New Zealand government's domestic and international obligations, especially human rights standards. Effective oversight is intended to support the agencies in this process, while at the same time recognising their lawful operational objectives.

---

<sup>12</sup> See e.g. ISA, ss 67, 68 and 69.

## Key requirements for effective oversight

As I have noted in previous annual reports there are some factors that are essential to effective oversight which can give confidence to the public. Independence is the critical factor. There are some formal protections for that independence:

- The Inspector-General is an independent statutory officer. The office was first constituted under the Inspector-General of Intelligence and Security Act 1996 and is continued under the ISA.
- The Inspector-General is organisationally separate from the agencies for which the Inspector-General has oversight, the NZSIS and GCSB. There is no reporting line to the agencies.
- The funding for the remuneration of the Inspector-General and the Deputy Inspector-General is through a Permanent Legislative Authority (PLA), which means that funding for that purpose can be changed only by Parliament and cannot be reduced for political reasons. The actual rate of pay is set by an independent body, the Remuneration Authority.
- The Inspector-General is not subject to direction from the Minister responsible for the intelligence and security agencies, the Prime Minister or other Ministers, on how the Inspector-General's responsibilities under the legislation should be carried out. The responsible Minister, the Prime Minister and the Intelligence and Security Committee can request that the Inspector-General undertake an inquiry but cannot compel her or him to do so. Nor can they require that an inquiry be halted.
- The appointment and removal provisions all support that independence. The Inspector-General and Deputy Inspector-General are appointed by the Governor-General on the recommendation of the House of Representatives, after the Prime Minister has consulted the Intelligence and Security Committee (ie there is cross-party consultation). The appointment is for a fixed term (maximum five years). The Inspector-General may be reappointed for one further term (maximum three years). The Deputy IGIS may be reappointed for one or more further terms.
- The process for removal of the IGIS is by the Governor-General, on an address from the House of Representatives. The grounds for removal<sup>13</sup> are similar to those for Judges (incapacity, bankruptcy, neglect of duty, misconduct, failure to hold the appropriate security clearance).

Other aspects that support the formal, legislative safeguards of independence are as follows.

*Mandatory public reporting:* annually and of specific inquiries, is an important aspect of effective oversight and of public accountability of the overseer. Public reporting is required by the ISA<sup>14</sup> and the Inspector-General may publish the Office's annual work programme.<sup>15</sup>

My approach has been to enhance transparency by publishing my reports or summaries of them even when I am not required to by law, and to encourage the agencies themselves to put as much material as possible in the public domain.

---

<sup>13</sup> ISA, sch 3, cl 8.

<sup>14</sup> ISA, s 188.

<sup>15</sup> ISA, s 159(3)(b).

*Access:* total, unmediated access to all security records (defined very broadly in the ISA to essentially cover all information held by the intelligence and security agencies) is essential for effective oversight.

Generally, accessing material involves a process of consultation and discussion with agency staff, but ultimately it must be for the Inspector-General, rather than the agency Director-General, to decide what information the Inspector-General should see.

*Resources:* sufficient, appropriate resources are essential. My predecessors lacked adequate resources. Until my appointment in 2014 the Inspector-General role was part-time, filled by a retired Judge, supported by a part-time executive assistant. The Inspector-General had no investigative assistance. Their independence of mind was not in question, but their ability to exercise it meaningfully was seriously compromised.

We are in a stronger position now, but still small and will need to augment our staff over the next few years. Currently the permanent staff of the office comprises the Inspector-General, the Deputy Inspector-General, 3.5 Investigators, an Office Manager/Executive Assistant and an IT Manager/Security Advisor.

*Own-motion jurisdiction and investigative powers:* dealing with complaints, reviews of operational activity and review of all warrants issued to the agencies work are the bread and butter of the Inspector-General's work, but the ability to initiate an inquiry into the legality or propriety of agency activities, where that is in the public interest, and without the need for government request or concurrence, is essential for the independence and perception of independence of the office. That ability is protected in the legislation.<sup>16</sup>

## **Measures of effectiveness**

In previous annual reports I noted that the effectiveness of the Inspector-General's office can be assessed against four key measures:

- the breadth and depth of inspection and review work
- the time taken to complete inquiries and resolve complaints
- the extent to which the agencies, Ministers and complainants accept and act on the Inspector-General's findings and recommendations
- the extent to which there is a change to the agencies' conduct, practices, policies and procedures as a result of the work of the Inspector-General's office.

### **Breadth and depth of inspection and review work**

While, as noted above, the IGIS office is much better resourced than five years ago, our limited resources relative to the agencies'<sup>17</sup> means that we have to consider carefully the balance between

---

<sup>16</sup> ISA, s 158

<sup>17</sup> In 2015 I noted publicly that the IGIS had the equivalent of approximately 1% of the staff and budget of the agencies we oversee. That percentage is not mandated by policy or legislation and in fact, as the agencies have gained resources, the percentage has fallen.

comprehensiveness of investigation and reporting and timely identification and reporting of key issues. The thoroughness of our reports to date, with corresponding production times, has helped to build public understanding of our role and of the work of the agencies. That thoroughness is also driven by fairness to the agencies, considering that they are limited in the extent to which they can put their own position publicly where that would disclose sensitive information about their work. In view of our limited size, we will need to think more in the future about whether it will be most effective to identify a key issue with an agency activity and highlight that promptly, or cover a topic more exhaustively.

### Time taken to complete inquiries and resolve complaints

All but two of the complaints received during 2017/18 were completed within a maximum period of four months.<sup>18</sup> Two complaints which involved more complex matters took eight and 11 months respectively to complete.

During this period we have also worked hard to complete some inquiries and reviews that have taken longer than anticipated and have largely done so. These are covered below.

As noted above, sometimes a choice must be made between intensive inquiry with a lengthy report, and a more focussed and brief inquiry.

### Extent to which agencies, Ministers and complainants accept and act on the Inspector-General's findings and recommendations

The written reports I prepare on completion of my inquiries (including inquiries into complaints) contain my conclusions and recommendations.<sup>19</sup> I also prepare reports on my operational reviews and these frequently include recommendations for the relevant agency.

I maintain an internal register of all the recommendations I have made to the NZSIS and the GCSB in my various reports. I monitor the agency implementation of those recommendations and regularly discuss their progress with the agency and the reasons for any delay in implementation.

I am able to advise the Minister responsible for the agencies about agency compliance with my recommendations and the adequacy of any remedial or preventative measures taken by an agency following an inquiry.<sup>20</sup> To date I have not had to take the step of formally reporting that an agency has declined or failed to implement any of my recommendations.

Examples of my findings and recommendations positively influencing the agency's activities include the Service's speedy and thorough response to my review of a self-reported compliance incident, involving inadvertent collection of data (referred to at p 18 below); the Bureau audit of New Activity Customer Requests to identify whether a proposed government intelligence requirement is recorded (as recommended in my report on GCSB's process for determining its foreign intelligence activity); and the Service's collaboration with the Human Rights Foundation on a fact sheet about rights when

---

<sup>18</sup> See more detailed statistics in the complaints section of this report.

<sup>19</sup> ISA, s 185.

<sup>20</sup> ISA, s 186.

dealing with the NZSIS, which arose out of my Inquiry into legality and propriety of warnings given by the NZSIS report.

### **Extent to which agencies' conduct, practices, policies and procedures change**

There are many discrete examples of where the work of my office has prompted changes in individual policies or practices. These include the examples noted below.

As a result of our consistent feedback to the agencies on their warrant applications, they have both made changes to their drafting templates and approach. The improvements to the structure, logical flow and readability of the applications has been significant. These changes assist the Minister and Commissioners of Intelligence Warrants in scrutinising the applications and issuing warrants, benefit agency staff working under the warrant, and assist my oversight.

The Service consulted my office on draft direct access agreements with Customs and Immigration and amended the drafts in response to our comments and questions.

The template for business records approvals and the register of business records approvals<sup>21</sup> were significantly revised after comment from my office.

### **Statutory advisory panel**

The principal role of the statutory advisory panel is to provide advice to the Inspector-General. While the advisory panel does not itself have an oversight role, the isolated nature of the Inspector-General's role means it is very valuable for her or him to have access to the independent perspective offered by the statutory advisory panel members.

After a lengthy period where no panel was in place, a new panel was appointed, with effect from 28 May 2018, with Angela Foulkes as Chair, for a period of two years and Lyn Provost for a period of five years. Both have extensive experience of the public sector, and I look forward to working with them.

### **Intelligence and Security Committee**

The ISC may consider and discuss with the Inspector-General his or her annual report as presented by the Prime Minister to the House of Representatives.<sup>22</sup> The Inspector-General may, with the agreement of the Prime Minister, report either generally or in respect of any particular matter to the ISC.<sup>23</sup> At the ISC's invitation I appeared before it on 20 February 2018 to discuss my 2016/17 annual report.

---

<sup>21</sup> ISA, pt 5, subpt 4.

<sup>22</sup> ISA, s 193(1)(g).

<sup>23</sup> ISA, s 222(8).

## THE YEAR AHEAD

### Work programme

The ISA requires me to prepare a draft proposed work programme each year. In preparing that draft I consult with the agencies. This allows us to agree respective priorities, resourcing requirements, and the scope and description of the work. I must also consult the Minister(s) responsible for the agencies.<sup>24</sup>

On 28 June 2018 I made public the office's detailed programme of work.<sup>25</sup> This is consistent with my general approach to provide as much information as possible to the public about the work of my office, to promote a better understanding of what the intelligence and security agencies do and ensure that I am accountable to the public in my oversight role.

The work programme describes the specific inquiries and reviews that my staff will undertake in the 2018/19 year. As for this reporting year, I expect that, in addition to those specific projects, much of our work will be reviewing the way in which the agencies are implementing the ISA.

---

<sup>24</sup> ISA, s 159(1)(b).

<sup>25</sup> See <http://www.igis.govt.nz/assets/Uploads/Work-Programme-2018-19.pdf>.

## INQUIRY AND REVIEW POWERS

### Inquiries

The Inspector-General can inquire into GCSB and NZSIS compliance with the law and into the propriety of particular agency activities.<sup>26</sup> The Minister, Prime Minister and ISC may request that I undertake an inquiry, or I may initiate an inquiry of my own volition.

The factors I consider when deciding whether I will initiate an inquiry include:

- Does the matter relate to a systemic issue?
- Are a large number of people affected by the issue?
- Does it raise a matter of significant public interest?
- Would the issue benefit from the use of formal interviews and other powers that are available in the context of an inquiry?
- Are recommendations required to improve agency processes?
- Is it the best use of my office's resources?

In the context of an inquiry the Inspector-General can use strong investigative powers akin to a Royal Commission, such as the power to compel persons to answer questions and produce documents and to take sworn evidence. I also have a statutory obligation to publish a report on every inquiry I undertake.

### Operational reviews

Reviews of operational activity form part of my office's regular programme of review of agency compliance systems.<sup>27</sup> While in rare cases a review might prompt a more formal inquiry, in general reviews are less formal and are aimed at strengthening agency practice and legal compliance. At the end of each review I provide a report to the agency Director-General and, in significant matters, the responsible Minister. I publish a summary of the outcome of each review, either in the relevant annual report, or as a stand-alone document.

---

<sup>26</sup> ISA, s 158.

<sup>27</sup> ISA, s 158(1)(f).

## INQUIRIES AND REVIEWS CONCLUDED IN 2017/18

### **Review of the NZSIS handling of privileged communications and privileged information**

This review was completed in June 2018, with my classified Report provided to the Directors-General of both intelligence and security agencies, and to the Minister. I reviewed the protections provided in the Service's policy and practice for the privileged communications and privileged information of New Zealand citizens and permanent residents.

I considered whether these protections accord with the relevant legislation, common law and related Ministerial Policy Statement. Informing my review was the principle that the privileges and protections for confidences in the Evidence Act 2006 reflect fundamental values in New Zealand society, with a recognised social value in having certain confidential relationships protected to a high degree from third party interference, including by the State. Legal professional privilege, in particular, holds a special position in the law. I reviewed in detail some 19 relevant Service policies, procedures, templates and training modules, relating to warranted activities. I also reviewed activities conducted without warrant, including the handling of inadvertently obtained or unsolicited privileged information. I sought comments from Service staff, including in response to a draft report.

My Report reflects the policy positions held by the Service (and to some extent the Bureau, given the joint application of the ISA), including where we differ on interpretations of law, principle and propriety. My recommendations relate to improving and clarifying operational policies, to assist staff with identifying and protecting privileged material across agency activities. I expect to publish a public report before the end of 2018, setting out the legal issues considered in this review and including a summary framework of my analysis of the agencies' obligations with respect to privilege under the new Act. The summary establishes for my office a template with regard to privilege, for use in future reviews of agency warrants and other activities, and will also provide transparency on what the law in this area means for the agencies.

### **Review of the New Zealand security classification system**

In 2017 I began a review of the New Zealand Security Classification System, the policies and rules that govern identification, marking, handling and access to sensitive official information. The aim was to identify possible improvements to the system which, like classification systems elsewhere, is often criticised for being difficult to understand and apply. My review was conceived as an independent input to a broader review of protective security policies being led by the Department of the Prime Minister and Cabinet (DPMC) and the NZSIS.

I completed the report of my review in November 2017, and published it in September 2018.<sup>28</sup> My report recommends a simplification of the classification system, reducing the number of classifications from six to three. The lowest, 'Protected', would be for sensitive information that can be held and transmitted on common internet-connected government information systems. Two higher

---

<sup>28</sup> See [www.igis.govt.nz/assets/Uploads/Classification-Review-Report.pdf](http://www.igis.govt.nz/assets/Uploads/Classification-Review-Report.pdf)

classifications, 'Secret' and 'Top Secret', would be for highly sensitive information needing the special protection of information systems isolated from the internet. A key objective of simplification would be to make correct classification easier, reducing over-classification and aligning classification with the way modern digital information systems work. My report also recommends a new approach to systematic declassification of historic classified records, focused on topics of interest.

Any change to the classification system would require broader consultation with affected users than I was able to undertake and will ultimately be a decision for Cabinet. In that context my report is a resource for the policy process being led by DPMC and NZSIS, not a set of recommendations they are obliged to implement. I think nevertheless that there is a strong case for updating and simplifying the classification system – and for a revised approach to declassification – and I will be taking a close interest in the approach the agencies adopt.

### **Inquiry into complaints regarding alleged GCSB surveillance in relation to the South Pacific**

In 2015 there was extensive news media coverage of alleged GCSB intelligence gathering activity in the South Pacific, based on what were alleged to be classified United States National Security Agency (NSA) documents disclosed by Edward Snowden. In consequence I received a number of complaints against the GCSB from people concerned that their private communications might have been intercepted. I began an inquiry into those complaints and a concurrent review of the Bureau's procedures and systems relevant to its activities in relation to the South Pacific during the period at issue (2009-2015). The guiding questions included whether the GCSB undertook "full take" collection of communications and, if so, what that meant, as this was a prominent question in the news media coverage and complaints.

My report<sup>29</sup> found that the GCSB undertook signals intelligence-gathering in relation to New Zealand's interests in the South Pacific during 2009-2015, including the collection of satellite communications. It did so under statutory authorisations and subject to policies and procedures governing its foreign intelligence activities. I found no evidence that GCSB acted outside the relevant authorisations and statutory prohibitions to any significant extent: two inadvertent breaches were detected and remedied. I found no evidence that the GCSB deliberately targeted the private communications of any complainant for collection. It was possible that some private communications of some complainants were collected incidentally, either through the use of collection methods that inherently involved the acquisition of some non-targeted communications, or if those individuals had any communications with targeted persons or organisations. If that occurred, I found no evidence that GCSB retained any data relating to any complainant. I found it unlikely that any data relating to any complainant's communications was shared by GCSB with a partner intelligence agency in another country, given the targeted nature of such sharing and access and the safeguards against unauthorised access to the private communications of New Zealand nationals.

I made no recommendations as a result of my inquiry and review, due to the absence of any adverse findings in relation to the complaints and the fact that the GCSB policies and procedures reviewed applied to operations under the GCSB Act 2003. Those have largely been superseded by new versions

---

<sup>29</sup> See [www.igis.govt.nz/assets/Uploads/GCSB-Intelligence-Activity-re-South-Pacific.pdf](http://www.igis.govt.nz/assets/Uploads/GCSB-Intelligence-Activity-re-South-Pacific.pdf)

designed for compliance with the ISA. The inquiry did however provide my office with a deep insight into GCSB processes, which continues to inform our approach to other inquiries and reviews. The report significantly expands the publicly available information on the Bureau's activities.

### **Review of NZSIS Requests made without warrants to financial service providers**

I provided the NZSIS in November 2017 with a draft report of my review of the Service's practice of requesting banks to voluntarily provide it with customer records. During this reporting year the NZSIS provided comment on the draft report, and worked to substantially improve its policies in this area as part of ISA implementation. The final classified version of the report was provided to the Director-General of the NZSIS in early August 2018. I intend to also publish an unclassified version of this report before the end of 2018.

While my review concerned NZSIS operational practice carried out under the New Zealand Security Intelligence Service Act 1969, most of the legal and propriety considerations addressed in the report remain relevant factors under the ISA. These include the role of s 21 of the New Zealand Bill of Rights Act 1990 (the right to be free from unreasonable search and seizure) when the Service is choosing which legal mechanism, within the ISA framework, should be used to seek personal banking information and the need for robust assessments of proportionality in determining the proper scope of requests. I considered the Service's responsibilities to banks, which in turn have a general duty of confidence to their customers, and I examined obligations under the Privacy Act 1993 and the Public Records Act 2005.

My recommendations reflect these matters. With respect to transparency I recommended, after consultation with the Privacy Commissioner, that the Service keep a record of all requests made to financial institutions to assist my oversight function and to enable the type and frequency of requests for disclosure of information to be monitored. The NZSIS is considering its final response to my three formal recommendations and what their implementation would involve.

### **Review of the inadvertent collection of Advance Passenger Processing information in relation to Persons of Interest**

As part of its self-reporting process, the Service notified me of the over-collection of Advance Passenger Processing (APP) data involving personal travel information about individuals who were not relevant to the statutory functions of the Service. As a result of this notification, I reviewed the context in which the over-collection had arisen and the remedial steps that had been taken. I also consulted with the Privacy Commissioner. In response to the issues raised by my review, the Service provided me with a comprehensive remedial plan, which I endorsed. This has now been implemented and completed. I was impressed by the speed and thoroughness of this work.

### **Inquiry into legality and propriety of warnings given by the NZSIS**

The previous Inspector-General, Hon Andrew McGechan CNZM QC, had dealt with a number of complaints concerning certain types of formal "warnings" given in writing by the NZSIS to a few individuals about particular behaviour and its possible legal consequences. In June 2014, shortly after I was appointed to this role, I commenced an inquiry into the NZSIS's broader practice of giving warnings. I examined whether there was a legal basis for the Service to direct the behaviour of any

person given that under the NZSIS Act in force at the time (and under the present Act) the Service does not have enforcement powers, and I assessed examples of any warnings given by the Service and the internal processes and policies governing that practice. My report<sup>30</sup> was finalised and published in December 2017.

I concluded that there was a fine line between NZSIS officers legitimately attempting to influence behaviour, and conduct that was, or might reasonably appear to be, in the nature of enforcement. I made detailed recommendations concerning changes that should be made to internal guidance for staff to ensure that officers do not overreach in this area. In particular I recommended clearer information be provided to members of the public about the Service's role and the voluntary nature of any meetings or discussions with the Service. The substance of most of my recommendations was accepted by the Service, and I was especially pleased that steps were taken promptly in early 2018 to implement the recommendations that had been accepted.

The key point for the NZSIS to take from this review concerns the duty to be clear that officers do not misrepresent, including inadvertently, the Service's role and the limits on it. To the extent some recommendations were not accepted, I am of the view that there remains scope for the Service to take more account of the nature of the information that it would be helpful for members of the public to have. For instance, I continue to encourage the Service to make it clear on their website and in their information sheets that the choice rests with anyone who agrees to engage with the NZSIS, on any matter, to have a lawyer or interpreter or other person present if they wish. At the same time I am aware that the Service in this reporting year cooperated with the Human Rights Foundation when the Foundation produced a guide to rights when dealing with the NZSIS, to enhance public understanding of the Service's role and the rights of individuals. I understand from engagement with the New Zealand Muslim community, that there has been a need for better information.

### **Review of the lawfulness of NZSIS access to data under the Customs and Excise Act 1996 and the Immigration Act 2009**

My report on the lawfulness of NZSIS's long-standing direct access to the Customs database, CusMod, and on its current ability to store and use Advance Passenger Processing information which it had obtained directly from an Immigration database, was published in December 2017. My conclusion, now accepted, was that the Service had no legal basis to access CusMod. In the circumstances, a positive legal power was required. I put a tight three month timeframe on the Service for implementation of my three recommendations. By contrast to the review process, the NZSIS's response to my completed report was beyond reproach. The agency comfortably met the three month deadline, while meantime keeping me updated on progress in completing the internal policy work and the other changes required to give effect to my recommendations. The Service acted on my recommendation to consult with the Privacy Commissioner to obtain advice about the unlawfully obtained CusMod data. I have seen and am satisfied by the careful and conservative processes it has put in place with respect to the historically obtained APP information. My office in 2018 had a number of informative and frank meetings with the Service's legal and compliance teams in respect of these matters.

---

<sup>30</sup> <http://igis.govt.nz/assets/Inquiries/Warnings-Report.pdf>

## ONGOING INQUIRIES AND REVIEWS

### **Inquiry into possible New Zealand engagement with Central Intelligence Agency (CIA) detention and interrogation 2001-2009**

I commenced this Inquiry in 2015, following the publication in December 2014 of the US Senate Committee on Intelligence’s executive summary of the CIA’s detention and interrogation programme. The torture and inhumane treatment that formed part of the CIA’s ‘Enhanced Interrogation Techniques’ has been well documented.

A focus of my Inquiry has been on whether the New Zealand intelligence and security agencies knew about or were otherwise connected with, or risked connection to, the activities discussed in the Senate report, during the period September 2001 to January 2009. The terms of reference for my Inquiry are also forward-looking, including an analysis of whether the agencies now have in place adequate safeguards to guard against the risk of unlawful behaviour, including the risk of complicity in torture carried out by a partner country. Internationally, concerns around this remain current and significant.<sup>31</sup>

This Inquiry has required considerable resources, not least identifying and evaluating the agencies’ relevant activities and records over the period 2001 to 2009. Substantial progress was made over the past year. The agencies’ formal responses to the legal analysis in my preliminary “discussion paper” of April 2017, were received over the period August 2017 to June 2018. We reviewed new Ministerial authorisations for information-sharing and a joint policy statement developed under the ISA. I interviewed the former Directors of the GCSB and the NZSIS for the period covered by the inquiry. This completed the fact-finding aspects of my Inquiry. My draft classified report was provided to the agencies and other affected parties on 30 July 2018 for them to comment on matters of factual accuracy and completeness and to respond to any potentially adverse conclusions or recommendations. Once this process is completed I will publish a shorter public report on the findings and recommendations of my Inquiry.

### **Review of a sample of NZSIS recommendations in respect of citizenship and immigration**

One of the NZSIS’s statutory functions<sup>32</sup> is to make recommendations to the Department of Internal Affairs under the Citizenship Act 1977, and to Immigration New Zealand under the Immigration Act 2009, to the extent there are matters relevant to security. I initiated a review of these functions in the previous reporting year. For a number of reasons, including the change to the governing legislation, my review was deferred. It is now included as part of the 2018/19 work programme.

The review will address the effectiveness and appropriateness of NZSIS procedures, compliance systems, policies and practices relevant to these statutory functions.

---

<sup>31</sup> See, for example, the two reports of the UK Intelligence and Security Committee of Parliament, published in June 2018: [Detainee Mistreatment and Rendition: 2001-2010](#); [Detainee Mistreatment and Rendition: Current Issues](#)

<sup>32</sup> ISA, s 11; previously NZSIS Act, s 4(1)(bc).

## **Review of sample of NZSIS security clearance decisions**

The NZSIS has a statutory mandate to conduct inquiries into whether particular individuals should be granted security clearances and to make appropriate recommendations based on those inquiries.<sup>33</sup> This review will examine a specified number or proportion of adverse and qualified security clearance decisions over a specified period.

We initiated but did not complete this review during the reporting year. It is now part of the 2018/19 work programme.

## **Afghanistan inquiry**

In March 2018 I commenced an Inquiry into the role, if any, of the GCSB and the NZSIS in relation to certain specific events in Afghanistan. Earlier preliminary enquiries by my office, following the publication of the book *Hit and Run* by Nicky Hager and Jon Stephenson, indicated a sufficient public interest justifying the commencement of a focused own-initiative inquiry. Events relating to Operation Burnham are within the scope of this Inquiry, as are certain United Nations Assistance Mission to Afghanistan reports and activities by others regarding detainees. The Inquiry's full terms of reference are available on the IGIS website.<sup>34</sup> It continues as part of my 2018-19 Work Programme, with the predominant focus to date on research and fact-finding. I anticipate completing the Inquiry by June 2019.

As I confirmed at its commencement, this Inquiry is not considering the actions and conduct of the New Zealand Defence Force, although some specific events and questions of fact may be common to my Inquiry and the Government Inquiry into Operation Burnham announced in April 2018. I have been exploring how the Inquiries might best cooperate, as necessary, while preserving the independence of our separate investigations.

## **Review of Warrants issued under the Intelligence and Security Act 2017**

I have completed my review and will publish my report shortly after this annual report. My objective with this review was to assess the agencies' approach to the applications they put forward for intelligence warrants against relevant policy objectives behind the new Act. My report was written from the outset with a view to publication. Some specific matters arising from the review are discussed in the sections of this annual report dealing with warrants and authorisations and compliance.

---

<sup>33</sup> ISA, s 11(3)(a)(i).

<sup>34</sup> See [www.igis.govt.nz/assets/Uploads/Inquiry-Terms-of-Reference.pdf](http://www.igis.govt.nz/assets/Uploads/Inquiry-Terms-of-Reference.pdf)

## COMPLAINTS HANDLED BY THE OIGIS IN 2017/18

Any employee or former employee of the GCSB or NZSIS<sup>35</sup> or any New Zealand person may complain to my office that they have or may have been adversely affected by an act, omission, practice, policy or procedure of the GCSB or NZSIS.

In many cases complaints or inquiries can be dealt with quickly and efficiently at an administrative level without the need for formal inquiry, which requires notification of the complainant's details to the Director-General of the agency complained about. In other cases, preliminary inquiries may reveal that an inquiry into the complaint is unnecessary.<sup>36</sup>

| Complaints by agency and source                        | GCSB     | NZSIS     |
|--|----------|-----------|
| <b>Number of complaints</b>                            | <b>9</b> | <b>17</b> |
| From members of the public                             | 9        | 17        |
| From intelligence agency employees or former employees | 0        | 0         |

### Description of the complaints and inquiries

A substantial proportion of the complaints received in this reporting year were from members of the public who believed that one or both of the agencies had undertaken surveillance against them. Other complainants were concerned that the agencies had used some kind of weapon against them. In each case, at my request, the relevant agency confirmed to me or to the complainant that it held no information about him or her. I was able to independently verify the correctness of those assurances.

Other complaints were more accurately characterised as requests for personal information under the Privacy Act 1993 or information under the Official Information Act 1982. Depending on the particular circumstances, these complainants were generally advised to make a request to the relevant agency with a right of complaint to the Privacy Commissioner/Ombudsman or Inspector-General if they were dissatisfied with the agency response. In a few cases I decided that the most efficient and speedy resolution of the matter would be achieved by my office maintaining the complaint and conducting preliminary inquiries.

Of the other two complaints received this year, one concerned a recommendation by the NZSIS to another government agency to decline to grant a security clearance to an employee of that agency. Another was a complaint as to whether the NZSIS had a proper statutory basis for undertaking alleged action in respect of the complainant. Following an inquiry by my office the first complaint was not upheld. The second was not completed as at the date of this report. I also completed inquiries this year into complaints received in previous years. None of these inquiries resulted in adverse findings against the agencies. The most significant complaints in this category are those described in my

<sup>35</sup> Although generally they have to exhaust any internal complaints procedures before the Inspector-General has jurisdiction.

<sup>36</sup> ISA, s 174.

published report on *Inquiry into complaints regarding alleged GCSB surveillance in relation to the South Pacific*.

The time taken over the year in review to deal with those matters that were accepted and investigated as formal complaints ranged from one week to eleven months. All but two were completed within four months.

## WARRANTS AND AUTHORISATIONS

Both the NZSIS and the GCSB are required to keep a register of all intelligence warrants issued to the Director-General of the agency and certain specified information about those warrants. The Minister, Chief Commissioner for Intelligence Warrants (in respect of Type 1 intelligence warrants) and the Inspector-General may access the register at any time.

In practice, each agency advises my office when a new warrant has been authorised and makes the warrant, the application for the warrant and any supporting documentation available for inspection and review by my staff.

I will report separately<sup>37</sup> on how intelligence warrants were sought and issued under the first nine months of operation of the ISA so I do not include that detail here.

In this reporting year my staff reviewed the following warrants in respect of each agency:

### GCSB

- 33 access authorisations and 13 interception warrants issued under s 15A(1)(b) and s 15A(1)(a) of the GCSB Act, respectively
- 19 intelligence warrants approved under the ISA, of which ten were Type 1 and nine were Type 2.

During this period the Bureau did clear the backlog of “historic” questions from my office arising from our warrant reviews, responding in writing to each of our queries. The Bureau seeks to provide reasoned answers to our questions, and the organisational effort behind the responses is visible. I appreciate their commitment to this process; it has allowed both of us to focus attention on the more recent warrants.

As to warrants under the ISA, I acknowledge in my separate Warrants report that a new legislative regime will often lead to interpretation questions and disagreements, resulting in a period of uncertainty. I am not critical of that situation per se, but the Bureau’s initial unwillingness to discuss their interpretative approach with my office prior to seeking new intelligence warrants under the ISA was unhelpful. That is strictly their right, but the consequence of that approach is that some significant legal issues have been identified and engaged with too late in the piece.

The Bureau was prompt in obtaining advice from the Crown Law office on certain matters prior to the ISA coming into force, but on other matters it has been slower than ideal in seeking definitive advice or expressing a final view to me of its legal position. I do expect the Bureau to actively engage with my office earlier to discuss its view on how the law applies to operational questions, particularly when they are significant and/or novel. As I note in my Warrants report, I do appreciate that the application of the ISA’s warrant criteria to the nature of the Bureau’s work has special challenges. That is a reason for closer engagement.

---

<sup>37</sup> *Warrants issued under the Intelligence and Security Act 2017.*

As acknowledged, a period of uncertainty, discussion and even dispute, is not unusual when any new statutory regime is introduced. I am not the agencies' legal adviser, but I do need to understand their view of the law and their reasoning in order to carry out my role. In the next reporting year I expect the Bureau to have and apply, and be able to articulate to me, a clear view of what the ISA warrant regime requires, informed by Crown Law Office advice if necessary. Any continued period of uncertainty in how the Bureau approaches this question would make it increasingly difficult for me to be satisfied as to the adequacy of its compliance systems.

## **NZSIS**

- Nine domestic intelligence warrants issued under the NZSIS Act
- Two foreign intelligence warrants issued under the NZSIS Act
- Eighteen warrants issued under the ISA, 12 of which were Type 1 and six of which were Type 2
- Three practice warrants issued under the ISA.

As with the GCSB, I had a number of concerns about the Service's approach to the new ISA warrant regime. However, the Service has more recently demonstrated its willingness to constructively discuss warrant interpretation and drafting issues and to make quite significant changes to its warrant applications accordingly.

As with the Bureau, I expect that in the next reporting year the Service will have and apply a clear view of what the ISA warrant regime requires, informed by Crown Law Office advice if necessary. Any continued uncertainty as to how the Service is approaching the warrant regime, or other relevant law, would make it difficult for me to be satisfied as to the adequacy of their compliance systems. I can only assess the Service's approach to operational activities against my view of the relevant legal standards if the Service is able to provide me with thoroughly reasoned legal explanations for its approach.

## ASSESSMENT OF WHETHER COMPLIANCE SYSTEMS ARE SOUND

### Purpose of and approach to certification

I must certify in each annual report the extent to which each agency's compliance systems are sound.<sup>38</sup>

As I have noted previously, I apply a "positive assurance" approach which means that I:

- Examine what compliance systems and controls, such as relevant policies, safeguards and audit/oversight/error-reporting measures, are in place.
- Draw upon my office's ongoing review work, examine a sample of each agency's activities. Because of the large volume of decisions and operations, I cannot scrutinise all activities – with the exception of warrants and authorisations – at all times and must be selective about which activities to examine in depth.
- Apply a materiality threshold: that is, I have sought to focus on whether compliance systems are sound in substance, rather than insisting upon any particular or formal arrangement, and whether identified shortcomings are material.

Certification of the soundness of the agencies' systems is therefore not the same as certifying every decision and action of the agencies was lawful and proper. Rather, it is directed to how the agencies minimise the risk of illegality and impropriety through training, guidance and awareness for staff, planning and operating safeguards; ensuring that breaches are brought to light, through effective audit and other oversight mechanisms; and ensuring those breaches are addressed, both in the particular instance and so far as they may disclose systemic shortcomings.<sup>39</sup>

There is a close connection between my office's specific review and inquiry work, which examines the legality and propriety of particular actions and practices, and the agencies' own compliance systems. To the extent that our review and inquiry work identifies breaches or problems, that may well indicate inadequacies in internal compliance mechanisms. Conversely, where compliance mechanisms are robust, that should lessen the likelihood of breach and also support and assist the rigour and transparency of my office's review and inquiry work.

### Outline and assessment of GCSB compliance systems

#### My assessment

In last year's report I noted that further focus was required by the GCSB around timeliness in the areas of responding to my office's questions about warrant applications and completion of internal investigations into self-reported incidents.

---

<sup>38</sup> ISA, ss 158 (1)(f) and (h) and s 222 (2)(c).

<sup>39</sup> See, among others, Department of Internal Affairs *Achieving Compliance: A Guide for Compliance Agencies in New Zealand* (2011) 25ff.

As to timeliness, the need to respond promptly to concerns I raise about the scope of the Bureau's powers or its interpretation of law remains an area for focus. Compliance systems assume that the legal standards are clear. With respect to both agencies it seems to me that once a live question has been raised about the legality of any activity or policy approach, the agencies must prioritise and expedite their legal assessment of that matter. If I am to be confident of the adequacy of the agency's legal response, and the soundness of arrangements in place, close engagement with my office in that process will be necessary.

In relation to self-reported incidents, I am satisfied that, although some investigations take longer to complete than is desirable, in all cases any significant mistakes or problems are promptly identified and where immediate remedial steps are required that occurs.

**Overall, I certify that the GCSB has sound compliance procedures and systems in place.**

### Compliance framework & structure

GCSB has comprehensive and up to date policies and audit procedures. There is a strong culture of commitment to compliance and to reporting and learning from errors. Bureau staff in roles at all levels engage very constructively with my office. The GCSB has continued to consolidate its compliance framework and practice and the important role of its Compliance and Policy Team. They have done well in normalising compliance activity and in establishing their role as professional advisors, rather than activity gatekeepers. That is important because it reinforces the message that compliance with law and policy is an integral part of all operational activity and a fundamental requirement of all staff.

For both agencies their compliance teams spent a great deal of time and focussed resources on developing policies, including Joint Policy Statements, and training to underpin the ISA. While it meant they were to some extent not available for day to day compliance activities, this was an essential part of ensuring legal compliance on an on-going basis.

### Compliance audit practices

The GCSB has a Mission Compliance Audit Plan and the Compliance and Policy team now has a dedicated auditor. The senior leadership team of the Bureau approved a comprehensive 2017/18 Audit Plan. Not all of the planned audits were completed during the reporting year, in part because of diversion of resources to assist with implementation of the ISA. A number were, however, completed. They ranged from an audit of operational activity carried out under a particular authorisation to check whether the activity was compliant, proportionate and within the terms of the agreed controls in the authorisation, to a review of whether GCSB intelligence production aligns with New Zealand's National Intelligence Priorities (NIPs).<sup>40</sup>

While internal audits do not replace the need for my office to review selected operational activities, they are an important part of ensuring that the organisation is complying with the law and relevant policy. They can also sometimes provide a starting point for an independent IGIS review.

---

<sup>40</sup> This arose from a recommendation made in my report into *GCSB's process for determining its foreign intelligence activity*, June 2017.

## Self-reporting of incidents

As I have said previously, I regard the self-reporting of errors or other incidents as a sign of a healthy and mature organisation. Mistakes will inevitably occur in every organisation. What is important is that staff feel they can identify those mistakes without fear of reprisal. This allows steps to be taken to deal with the consequences of a particular incident as soon as possible and measures such as changes in policy and procedure and fresh training can be put in place to minimise future recurrences. The technical and complex nature of the Bureau's work makes this self-reporting function particularly important.

The GCSB uses a Compliance Incident Register to track and manage potential incidents discovered or reported during the course of operational activities where an incident involves possible breach of a policy, warrant or authorisation or of the governing legislation. The Compliance and Policy Team investigate the incident and follow a process to evaluate the nature, significance and risks of the incident, with escalating procedures to deal with it appropriately. Ensuing steps may include changes to policy, procedure and training.

The Compliance, Risk and Assurance team notify my office of their investigations into incidents and I am able to – and frequently do – query how the incident occurred and what subsequent remedial steps have been taken and make recommendations for further or different action, if I consider that to be necessary.

In this reporting year there were 13 self-reported incidents notified to my office by the Compliance team which became aware of them through either self-reporting by Bureau staff or partner agency audit. As at 30 June 2018, five historical (pre-2017/18) Compliance Investigations and three historical Compliance Surveys remained open, but a further six compliance surveys were launched during the 2017/18 year which have not yet been closed.

I am satisfied that the incidents were promptly reported and investigations commenced. In each case the incidents reflected inadvertence or factual or technical mistakes. I am also satisfied that any data inadvertently collected was deleted and any necessary training or changes to processes put in place.

## Interaction with IGIS office

The Bureau's compliance practices also incorporate scheduled and ad hoc engagement with my office, including:

- notification of self-identified compliance incidents, as above, as soon as practicable after those incidents occur. Where necessary, we discussed proposed investigative and/or remedial steps with the Compliance and Policy Manager and sometimes the Chief Legal Adviser
- occasional consultation with my office on novel or likely contentious actions or issues. While it would be inconsistent with my review and oversight role to provide prior "authorisation" for particular actions, consultation does provide an opportunity to avert obvious risk areas
- monthly GCSB/IGIS Working Group meetings. This Group was set up as a forum for the Inspector-General to discuss operational issues and processes, and compliance consequences, with

compliance and audit staff and relevant operational managers. It has evolved into a useful forum where senior Bureau managers can also brief me about changes or issues in their area, and

- occasional compliance and policy reports which cover the development of operational policies and procedure, compliance training of staff, audit activity, Official Information Act and Privacy Act requests.

There is also a compliance component to the Bureau's wider engagement with my office, through:

- regular meetings with the Director-General of the GCSB and his senior staff, including in regular joint meetings with the Director-General and senior staff of the NZSIS
- monthly meetings with the Chief Legal Adviser to discuss any questions or issues identified in our regular review of warrants and authorisations, and
- occasional consultation on draft policies and procedures.

## **Outline and assessment of NZSIS compliance systems**

### **My assessment**

In last year's report I noted two specific areas for the Service to address: first, the need to respond more quickly to oversight requests and second, the need to do whatever is necessary to be confident of a sound legal basis for all operational activity.

As to the timeliness in responding to oversight requests, in this reporting year both agencies have had a much more time-consuming programme of work around implementation of the ISA than they, or I, anticipated. For both agencies, as I noted elsewhere in this report, this has required developing a wide range of policies and procedures followed by training to ensure they are properly embedded. I acknowledge too that I have required the NZSIS to respond to a larger number of reports prepared by my office than is usual as I sought to complete some outstanding reviews and inquiries. It is fair to recognise that of the two agencies the Service had the greater burden of the work generated by my office's oversight.

I expect that, in the 2018/19 year, now that the work of implementing the ISA has been largely completed and the initial interpretation of some key warrant provisions of the ISA resolved, both agencies will be able to respond to my requests for information and clarification and to the substance of draft reports in a more timely manner.

As to the second reservation I expressed last year, the Service has demonstrated a much greater willingness to discuss contested legal issues frankly and at an earlier point, and to seek further advice if necessary, so it can be sure it is acting lawfully and properly.

I have noted above the progress made with the Service about intelligence warrant applications. In other compliance contexts too it has acted promptly on my recommendations to obtain specialist advice, for instance from the Privacy Commissioner.

**Overall, I certify that the NZSIS has sound compliance procedures and systems in place.**

### Compliance team

The NZSIS has continued to consolidate its Compliance and policy functions, with a fulltime Compliance Manager and a small compliance and policy team. This has assisted in the ongoing establishment of a stronger compliance culture.

### Compliance reporting

I have received regular reporting from the Service Compliance team on a bi-monthly basis. This has been supplemented by specific briefings where necessary and regular contact with the Compliance Manager to discuss operational compliance incidents (see below).

### Audit programme

In May 2017 the NZSIS implemented a Compliance audit plan to June 2018. Three audits were completed in 2017/18. Two audits were commenced in 2017/18 but completed after 30 June 2018 and one audit was commenced in 2017/18 and is still underway. The audits covered a range of operational activities as well as an assessment of agency compliance with general legislative requirements.

### Self-reporting of operational compliance incidents

This self-reporting function has become an established part of NZSIS operations and compliance. Such incidents are reported to me by the NZSIS Legal or Compliance team as soon as the incident becomes known to them. A full report is provided once an internal investigation of the incident is completed. At that point I have an opportunity to comment on the incident and the investigation, to ask questions and, if necessary, to make recommendations for remedial action.

A total of eleven incidents were notified to me in this reporting year. I was satisfied, sometimes after seeking further information or making suggestions as to remedial steps, that appropriate steps were taken in relation to each incident to mitigate the effect of the particular error and that overarching policies and processes were reviewed as appropriate.

One of the incidents notified to me involved the APP compliance incident mentioned at p18 of this report and is notable for the way in which the Service put in place a comprehensive remedial plan.

### Interaction with IGIS Office

My office's engagement with the NZSIS principally occurs by way of:

- regular meetings with the Director-General of Security, including in joint meetings with the Directors-General of both agencies and their senior staff
- regular meetings with the IGIS/NZSIS Liaison Group, which provides a useful, regular forum for me and the Deputy Inspector-General to meet with senior NZSIS staff to discuss current IGIS Office inquiries and reviews and emerging issues

- Monthly meetings with the Service's Chief Legal Adviser to discuss any questions or issues arising from the review of all warrants.
- Discussions with relevant operational staff and members of the Service's legal team on specific issues.

We have received a number of informative and useful briefings from the Service staff this year on operational matters, most of which have arisen from compliance incidents or from the implementation of recommendations from my operational reviews. In addition, we have had considerable technical assistance to aid our independent access to Service information.

## OTHER ACTIVITIES

### **Intelligence Oversight Group**

The Privacy Commissioner, Chief Ombudsman, Auditor-General and I meet regularly as the Intelligence and Security Oversight Coordination Group. Each of us has a role in oversight of the intelligence and security agencies and it has proved useful to discuss areas of overlap in our responsibilities and broader issues of common interest. It is important to develop relationships of mutual support, coordination and cooperation between integrity agencies. This helps each of us to maintain long-term independence. I have been grateful for the involvement of the Privacy Commissioner and his office in providing a fresh perspective, external to my office and the agencies, on a number of matters this year that arose in the context of particular operational reports.

### **Reference Group**

As I note in the foreword (at p 4 above), this year I invited a group of external individuals to join in discussions as an Inspector-General's "Reference Group" to help keep me up to date with external developments and thinking.

### **Visits to regional facilities**

Five members of my staff visited the Bureau's Waihopai facility in November 2017. Two members of my staff visited the NZSIS's northern regional office in January 2018.

### **Public engagements**

I look for opportunities for public engagement to talk about the Inspector-General's office because I think it is important to build public trust and confidence that we are scrutinising what the agencies do in a rigorous and independent way. We must ourselves be as transparent as possible. It is also important that we help to foster a public discussion about the role and activities of the intelligence and security agencies in New Zealand.

As at the date of publication of this report I had spoken at six meetings within the Intelligence Community, five other government agencies and a group of senior consultants and a group of lawyers. I was also part of a panel discussion on George Orwell's *1984* at the Auckland Arts Festival. The Deputy Inspector-General presented to an Intelligence Community conference, a team at the Ministry of Justice, and has spoken on a number of occasions at the Service's induction of new staff.

Shortly before this report was prepared the Deputy Inspector-General and I attended the third meeting of the Five Eyes Intelligence Oversight and Review Council (FIORC). FIORC comprises the non-political intelligence oversight, review, and security bodies from the United Kingdom, United States, Canada, Australia and New Zealand. The purposes of the forum include to exchange views on subjects of mutual interest and concern, compare best practices in review and oversight methodology, explore areas where cooperation on reviews and the sharing of results can occur and to encourage transparency to the largest extent possible.

## **Secondment**

In late 2017 we benefited from having a senior staff member of the Security Intelligence Review Committee (SIRC) (the oversight body responsible for overseeing and reviewing the operations of Canada's security service, the Canadian Security Intelligence Service) working in our office. In August 2018 that person commenced a one year secondment with us.

## OFFICE FINANCES AND ADMINISTRATIVE SUPPORT

### Funding

The IGIS office is funded through two channels. The first is a Permanent Legislative Authority (PLA) for the remuneration of the Inspector-General and the Deputy Inspector-General.<sup>41</sup> The second is the operating costs of the office which are funded from Vote: Justice (Inspector-General of Intelligence and Security) as part of the Ministry of Justice's non-Ministry appropriations.

### 2017/18 budget and actual expenditure

Total expenditure for the 2017/2018 year was \$1.451 million, as follows:

|  | Actual (\$000s) | Budget      |
|--|-----------------|-------------|
| Staff salaries/advisory panel fees; travel | 663             | 686         |
| Premises rental and associated services    | 82              | 106         |
| Other expenses                             | 60              | 105         |
| Earthquake Expenses                        | 0               | 0           |
| Non-Departmental Output Expenses (PLA)     | 606             | 570         |
| <b>Total</b>                               | <b>1411</b>     | <b>1467</b> |

### Administrative support

On-going administrative support, including finance and human resources advice, is provided to the Inspector-General's office by the Ministry of Justice. The New Zealand Defence Force provides standalone IT support, on a cost recovery basis.

---

<sup>41</sup> ISA, sch 3, c19.



**Office of the Inspector-General of Intelligence and Security**

P O Box 5609

Wellington 6140

04 817 0402

enquiries@igis.govt.nz

[www.igis.govt.nz](http://www.igis.govt.nz)

Follow us on Twitter @igisnz